Academic subject:
Cryptography

Degree Class: LM-40 - Matematica		**Degree Course:** Mathematics	**Academic Year:** 2018/2019
		Kind of class: Mandatory/Optional depending on the Curriculum	**Year:** | **Period:** 2
			ECTS: 7 divided into **ECTS lessons:** 6.5 **ECTS exe/lab/tutor:** 0.5

Time management, hours, in–class study hours, out–of–class study hours
lesson: 52
exe/lab/tutor: 8
in–class study: 60
out–of–class study: 90

Language: Italian	**Compulsory Attendance:** no		
Subject Teacher: Roberto La Scala	**Tel:** +39 080 5442674 **e–mail:** roberto.lascala@uniba.it	**Office:** Department of Mathematics Room 28, Floor 2	**Office days and hours:** Monday 11-13. Other days and times by appointment.

Prerequisites:
Mathematical knowledge which usually is acquired during the three years of a degree of L-35 class. Especially: arithmetics, algebraic structures and discrete probability.

Educational objectives:
Acquiring concepts and methods of modern cryptography.

Expected learning outcomes (according to Dublin Descriptors)

Knowledge and understanding:
Acquiring fundamental concepts in modern cryptography and related methods.

Applying knowledge and understanding:
The acquired theoretical knowledge is useful in the technology of information security.

Making judgements:
Ability to analyze the correctness of presented methods. Ability to identify appropriate mathematical tools and techniques to deal with information security issues.

Communication:
Students should acquire the computational language which is needed for understanding and developing methods, for analyzing and solving problems.

Lifelong learning skills:
Acquiring suitable learning methods, supported by the implementation of algorithms which are able to solve the exercises and questions periodically suggested during the course.

Course program
Classic cryptography, cryptanalysis. Shannon's information theory, perfect secrecy, information entropy, key-equivocation. Product ciphers, block ciphers, Data Encryption Standard, Advanced Encryption Standard. Public key cryptography, RSA cryptosystem, primality tests, square roots modulo n, factorization algorithms. Discrete logarithms, ElGamal's cryptosystem, computation of discrete logarithms. Applications of cryptography to digital signature.

Teaching methods: Lectures and exercise sessions.
Auxiliary teaching: Implemented algorithms in the programming language of SageMath.
Assessment methods: Oral exam.
Bibliography: D. Stinson, Cryptography: theory and practice, 3rd Edition, 2005 S. Vaudenay, A classical introduction to cryptography, Springer, 2006